

Compliance-Management-Systeme nach deutschem Standard

Anforderungen an Compliance-Strukturen helfen Haftung von Unternehmen und Management auf internationaler Ebene zu reduzieren

RA Dr. Christian Schefold*

Das Institut der Deutschen Wirtschaftsprüfer (IDW) hat am 11. März 2011 den IDW Prüfungsstandard (IDW PS 980) verabschiedet. Dieser Standard gibt „Grundsätze ordnungsgemäßer Prüfung von Compliance-Management-Systemen“ vor. Die endgültige Fassung ist das Ergebnis erheblicher Diskussionen nicht nur im Kreis der Wirtschaftsprüfer sondern auch innerhalb der betroffenen Wirtschaftsunternehmen sowie in der Anwaltschaft.

1. Einleitung

Eine Entwurfsfassung des IDW PS 980 war bereits ein Jahr zuvor mit der Bitte um Stellungnahme publiziert worden. Dieser Bitte wurde mit sachlichen und weniger sachlichen Eingaben gefolgt. In der Öffentlichkeit herrschte die ablehnende Haltung vor, dass dieser neue Prüfungsstandard vor allem dazu diene, der Zukunft der Wirtschaftsprüfer wieder mehr lukrative Mandate zuzuspielen.

Dieser Behauptung war in Deutschland zunächst wenig Stichthaltiges entgegenzusetzen. Es kam jedoch Schützenhilfe aus dem Ausland: Ein britisches Gesetz untermauert nun Sinn und Zweck eines einheitlichen Prüfungsstandards. Der *UK Bribery Act* wurde vor einem Jahr bereits vom britischen Parlament beschlossen. Er gilt nicht nur für britische Unternehmen sondern für alle in Großbritannien tätigen Unternehmen. Als Ergebnis von Eingaben der britischen Wirtschaft sah der Gesetzgeber eine Anleitung vor, nach der sich die Korruptionsprävention eines Wirtschaftsunternehmens richten sollte. Das Justizministerium in London war gefordert, die Grundlagen eines Compliance-Management-Systems zur Prävention gegen Korruptionsrisiken aus einer Unternehmenssicht heraus zu definieren. Ohne diese Anleitung (zutreffender Weise im Act als „Guidance“ bezeichnet) hätte das neue Anti-Korruptionsgesetz gar nicht in Kraft treten können.



Dr. Christian Schefold

2. Weltweit neue Entwicklung bei Compliance

Sektion 7 des *UK Bribery Act* sieht eine *strict liability* eines Unternehmens vor, aus dessen Reihen aktiv mit Hilfe von Korruption Geschäft generiert wird. Das Unternehmen ist für seine Geschäftsleitung, seine Mitarbeiter und seine Geschäftspartner ähnlich einer Gefährdungshaftung strafrechtlich haftbar, wenn es nicht die „Unabwendbarkeit“ einer solchen Tat aufgrund eines nicht vorherseh-

baren Versagens eines unternehmensinternen Präventionssystems nachweisen kann. Dieser Nachweis setzt ein funktionierendes CMS voraus. Die *Guidance* zum *UK Bribery Act* gibt hierfür einige Anhaltspunkte. Der *UK Bribery Act* beschränkt sich in seiner Wirkung nicht auf das Inselreich, sondern gilt gewissermaßen global. Ein deutsches Unternehmen mit Geschäftstätigkeit in Großbritannien muss die *strict liability* des Acts fürchten. Zum ersten Mal hat ein europäischer Gesetzgeber sich der Systematik der USA angeschlossen, Unternehmen selbst für Verhalten seiner Mitarbeiter straf- und ordnungsrechtlich haftbar zu machen, sofern sie nicht durch ein Compliance-Programm ernsthafte Präventionsanstrengungen glaubhaft machen können. Auch die Anwendung der §§ 130, 30 und 9 OWiG geht in Deutschland langsam aber sicher in dieselbe Richtung.

Damit haben Geschäftsleitungen einen berechtigten Grund, frühzeitig zu erfahren, ob die Vorkehrungen in ihrem Unternehmen ausreichen, um eine solche Haftung auszuschließen. Neben dem Aufbau eines geeigneten Compliance-Management-Systems ist daher auch eine Abnahme und Prüfung auf Geeignetheit dieses speziellen Risikomanagementsystems erforderlich. Hier setzt der neue Prüfungsstandard IDW PS 980 gerade rechtzeitig ein. Er bildet in Europa gewissermaßen die deutsche Ergänzung der britischen *Guidance* zum *UK Bribery Act*.

Doch nicht nur gesetzliche Anforderungen machen die Prüfung eines solchen Präventionssystems erforderlich. Insbesondere in der Automobilindustrie oder im Großanlagenbau werden Zulieferverträge oft nicht mehr ohne umfangreiche Compliance-Klauseln abgeschlossen. In derartigen Klauseln ist nicht nur das Verbot bestimmter Verhaltensweisen festgehalten und detailliert, mittlerweile enthalten diese Vertragsbestandteile auch umfangreiche Verpflichtungen zur Prävention gegen Wirtschaftskriminalität und insbesondere Korruption. Großkonzerne setzten zu ihrem eigenen Schutz die Verpflichtung zum Aufbau eines CMS ihrer Vertragspartner durch. Dabei beschränkt man sich nicht auf die reine Verpflichtung, Kontrollen werden vorbehalten. Will man nun eine Kontrolle durch die Außenrevision oder Beauftragte eines Auftraggebers vermeiden, ist es sinnvoll, eine Eigenkontrolle nachweisen zu können. Hier hilft der neue Standard, denn auch externe Prüfungen von Geschäftspartnern werden sich nach diesem Standard richten. Derartige An-

* Dr. Christian Schefold ist Rechtsanwalt im Berliner Büro von Mayer Brown LLP.

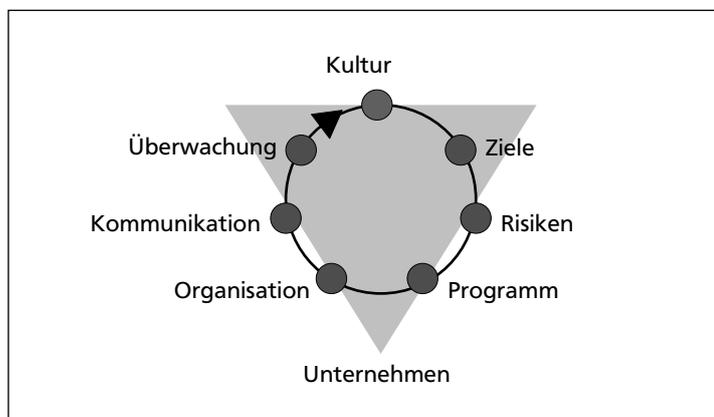


Abb. 1: Compliance-Elemente nach IDW PS 980

forderungen sind nicht nur auf Auftraggeber dieser Industrien beschränkt. Investoren, gleich ob fremdfinanzierende Banken oder Eigenkapitalgeber wie Investmentfonds, setzen mittlerweile auf ein Compliance-Management-System in ihren Investitionsobjekten. Gewisse Investitionen insbesondere mit einem rechtlichen Risikogehalt wie zum Beispiel eine Geschäftsexpansion in korruptionskritische Schwellenländer werden nur dann noch finanziert, wenn entsprechende Vorkehrungen glaubhaft und prüfbar getroffen wurden. Auch hier bietet der Prüfungsstandard IDW PS 980 eine gute Nachweisgrundlage. Nicht zuletzt ist ein erfolgreicher Prüfbericht über ein Compliance-Management-System mehr als hilfreich für einen erfolgreichen Börsengang, da er zukünftige Aktionäre vom Bestehen eines wirksamen Risikomanagementsystems gegen Compliance-Risiken überzeugen kann.

3. IDW PS 980

Was ist nun wesentlich am Prüfungsstandard IDW PS 980? Eine Arbeitsgruppe am Institut der Deutschen Wirtschaftsprüfer hat sich unterschiedliche Risikomanagement-Ansätze angesehen und diese auf ein rechtliches Risikomanagement übertragen. Damit wurde das noch neue Thema Compliance gleichzeitig dem Risikomanagement im Unternehmen zugeordnet und dem Bereich der Rechtsabteilung gewissermaßen entzogen. Hier entsteht im Prüfungsstandard ein gewollter Bruch. Der Wirtschaftsprüfer fühlt sich zwar dazu berufen, über Risiken und Ri-

sikopräventionsmaßnahmen in einem Unternehmen zu urteilen, das für die Bewertung eines Compliance-Management-Systems notwendige Knowhow kann er jedoch nicht in der erforderlichen Intensität und Qualität aufweisen. Es fehlt ihm am vertieften juristischen und rechtmetho- dischen oft aber auch geschäftstechnischen Wissen. Ohne die Hilfe von Rechtsanwälten und Brancheninsidern wird er Prüfung und Beratung nicht vornehmen können. Moderne Compliance-Management-Systeme stellen eine Querschnittsfunktion zwischen Risikomanagement, Revisions- und Controllingaufgabe, Unternehmens- und Rechtsberatung dar.

Gewissermaßen als Extraktion der Grundzüge unterschiedlicher Risikomanagement-Standards aus allen Teilen der Welt sieht IDW PS 980 sieben Elemente eines Compliance-Management-Systems vor: Kultur, Ziele, Risiko, Programm, Organisation, Kommunikation und Überwachung.

Während gesetzliche Vorgaben für ein Compliance-Management-System in Deutschland sich im Wesentlichen auf § 130 Abs. 1 OWiG beschränken und dabei allein auf Aufsichtsmaßnahmen zur Verletzung von Straftaten oder Ordnungswidrigkeiten – einschließlich der Bestellung, sorgfältigen Auswahl und Überwachung von Aufsichtspersonen – abstellen, gehen andere Rechtsordnungen darüber hinaus. Eine ausländische Vorgabe mit maßgeblichen Auswirkungen in Deutschland stellen die *Federal Sentencing Guidelines for Organizations* („FSGO“) der USA dar. Es darf erwartet werden, dass die Ende März veröffentlichte *Guidance* zum *UK Bribery Act 2010* bezüglich des Themas Korruptionsvermeidung bald eine ähnliche Rolle spielen wird. Seit 2001 definiert auch das italienische Gesetz Nr. 231/2001 organisatorische Anforderungen zur Verhinderung von Wirtschaftskriminalität und Arbeitsunfällen, Auswirkungen über Italien hinaus sind bisher jedenfalls kaum spürbar.

4. Der Standard im Vergleich zu US-Vorgaben

Die FSGO dient der Orientierung eines Gerichts oder einer Behörde bei der Beurteilung des Wohlverhaltens eines ehemals auf fällig gewordenen Unternehmens. Sie definiert Mindestanforderungen, an denen sich ein Unternehmen ausrichten muss, will es (Bewährungs-) Auflagen zur Verbesserung seines Compliance-Status erfüllen. Wesentlich ist die Ausrichtung auf Integrität und Compliance hin. Dies kann nicht allein durch eine Grundcharta (*Code of Conduct* oder Verhaltensrichtlinie) erfolgen sondern muss bereits eine wirkungsvolle Umsetzung beinhalten. Hier ist zum einen auf eine klar erkennbare und gelebte Selbstverpflichtung der Geschäftsleitung abzustellen. Zum anderen muss ein Compliance-Programm an unterschiedlichen Maßnahmen definiert und umgesetzt sein. Eine der wichtigsten Maßnahme stellt eine Compliance-Organisation dar, die sich um Richtlinien, Kommunikation, Kontrolle und Konsequenzen erfüllter oder nicht erfüllter Anforderungen kümmern muss. Auch hier wird dem Erfordernis fortschreitender Entwicklung durch das Postulat einer eigenen Überwachung und Verbesserung Rechnung getragen. So soll die Compliance-Organisation nach den Vorgaben der FSGO insgesamt die Unternehmenskultur prägen und in Richtung Integrität prägen helfen. Dabei können Grundcharta und Selbst-

verpflichtung der Geschäftsleitung als Synonym für Unternehmenskultur gesehen werden. Zieldefinition und Risikoanalyse – zwei weitere Elemente des deutschen Standards IDW PS 980 – ergeben sich hier aufgrund gesetzlicher Notwendigkeiten automatisch. Die FSGO ist auf die Korrektur von Gesetzesverfehlungen ausgerichtet. Ziele ergeben sich aus den gesetzlichen Anforderungen, Risiken haben sich in der Regel bereits verwirklicht.

5. UK Guidance als Anforderung und Maßstab

Die *Guidance* zum UK Bribery Act setzt primär auf eine Selbstverpflichtung der Geschäftsleitung („*top-level commitment*“) zur *Anti-Bribery Compliance*. Sie muss im Unternehmen auch ein zur Abwehr von Korruptionsrisiken im Verhältnis zu Unternehmensgegenstand, -größe und Risikosituation angemessenes Verfahren („*adequate procedures*“) einführen. Mindestens müssen Vorkehrungen zur Korruptionsprävention Maßnahmen zur sorgfältigen Auswahl von Personal und Geschäftspartnern sowie eine ausreichende Kommunikation und Schulung aller Betroffenen über Korruptionsprävention im Unternehmen vorsehen. Die Angemessenheit der Präventionsmaßnahmen wird sich im Regelfall aus einer Risikoanalyse ermitteln und im Rahmen der Erkenntnisse einer wirkungsvollen Überwachung optimieren. Verglichen zum Prüfungsstandard IDWPS 980 wird das Element Kultur durch die Selbstverpflichtung der Geschäftsleitung ersetzt. Eine Zielermittlung als weitere Voraussetzung für eine Ausrichtung des Compliance-Programms entfällt, da sich das Ziel aufgrund der Fokussierung auf Korruptionsprävention alleine bereits hinreichend definiert. In Großbritannien arbeitet man derzeit konzentriert an einem *British Standard*, der eine Prüfung von Compliance-Management-Systemen entsprechend der *Guidance* zum UK Bribery Act vorbereitet.

6. Compliance-Kultur – Basiselement für Compliance

Basis und wichtigstes Element eines Compliance-Management-Systems ist eine, auf Compliance ausgerichtete Unternehmenskultur. Das Selbstverständnis eines Unternehmens wird nicht ohne Wertmaßstäbe auskommen und es wird kein erfolgreiches

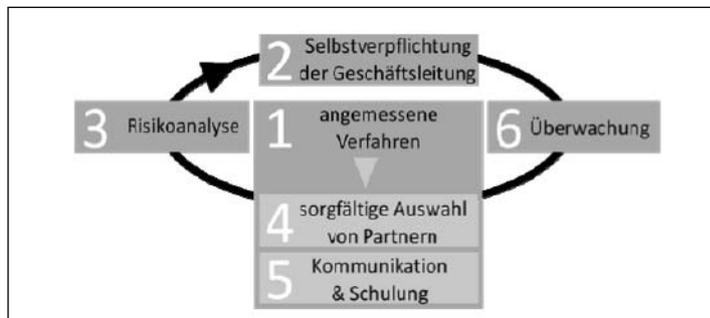


Abb. 3: Compliance-Elemente der Guidance zum UK Bribery Act

Wirtschaften geben, das auf rechtswidrigem Handeln und Rechtsverstößen aufbaut. Die Unternehmensskandale der Vergangenheit haben aber gezeigt, dass Unternehmenskultur oder das Verständnis von Unternehmenskultur durchaus Irrwege einschlagen und Integritätsbewusstsein allzu kurzfristigen Erfolgsstreben weichen kann. Wird eine Unternehmenskultur allein von einseitigen Erfolgskriterien beherrscht, kann die ethische Dimension verloren gehen. Die Unternehmenskultur definiert sich immer neu aus dem Unternehmen heraus, denn auch neue Entwicklungen eines Unternehmens schlagen sich in der Kultur nieder. Dabei beeinflusst ein Compliance-Management-System selbst die Unternehmenskultur. Ähnlich einem Regelkreis bestimmt die Unternehmenskultur die Elemente eines Compliance-Management-Systems und wird dabei durch dieses System auch wieder in den Aspekten einer Compliance-Kultur weiterentwickelt.

Aus der Unternehmenskultur sind Unternehmens- und Compliance-Ziele abzuleiten. Der nächste Schritt ist die Ermittlung des Status sowohl des Unternehmens als auch der einzelnen Einheiten im Hinblick auf die gewünschte Zielerreichung. Die Ursachen für eine mögliche Diskrepanz zwischen Status und Ziel stellen Compliance-Risiken dar, die der Zielerreichung entgegenstehen. Diese Risiken müssen erkannt und in ihrem Gefahrenmoment der Dringlichkeit, der Eintrittswahrscheinlichkeit und dem Ausmaß möglicher Konsequenzen für das Unternehmen nach beurteilt werden. Ein Compliance-Programm soll dann inhaltliche, organisatorische und weitere Maßnahmen zur Vermeidung des Eintritts dieser

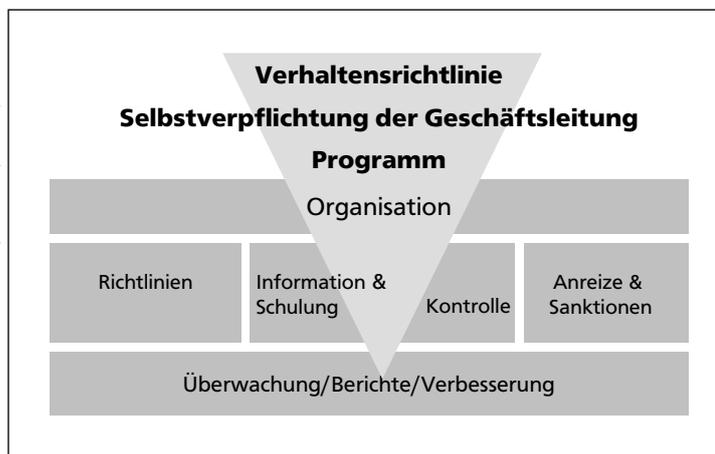


Abb. 2: Compliance-Elemente nach US-FSGO

Risiken definieren. Gleichzeitig werden diese Maßnahmen den Compliance-Status in Richtung Zielerreichung entwickeln. Für die Risikoevaluation und Maßnahmendefinition bedarf es einer fest definierten Zuständigkeit im Unternehmen: Dies ist die Compliance-Organisation. Zwei Maßnahmenbereiche sind für Compliance von erheblicher Bedeutung und zudem allgemein unabhängig von den jeweiligen Gegebenheiten in den einzelnen Unternehmensbereichen, so dass sie eigenständige Elemente eines Compliance-Management-Systems bilden. Es ist die Kommunikation als Basis der Transformation von Zielen und Maßnahmen in die Unternehmensorganisation und die Überwachung als stete Compliance-Statuserhebung, kritische Selbstprüfung und Grundlage der steten Anpassung und Optimierung von Compliance. Dieses letzte Element verdeutlicht den unmittelbaren Einfluss aller Elemente auf die Unternehmenskultur, die dadurch fortentwickelt und wieder einen Anstoß zur Weiterentwicklung geben kann. Dabei wird die Unternehmenskultur nicht nur von Compliance beeinflusst. In gleicher Weise führen Produkt- und Geschäftsentwicklung zu einer Fortschreibung und Anpassung des Unternehmens und bestimmen dabei auch die Anforderungen an Compliance und Integrität.

6.1 Compliance-Ziele

Während bei einem Compliance-Programm nach der *Guidance* die Zielrichtung von vornherein klar ist, erfordert der allgemeine Ansatz nach IDW PS 980 eine eigene Zieldefinition. Damit ist der Standard hoch flexibel, denn er erlaubt unterschiedliche und für das jeweilige Unternehmen genau angepasste Prämissen. Dies eröffnet die Chance, Compliance spezifisch auf das Unternehmen hin anzupassen. Zudem erlaubt der Standard eine Stufung der Ziele, in dem man eine Bewertung der Dringlichkeit einzelner Compliance-Themen für das Unternehmen durchführt und entsprechend Unternehmensressourcen sparsam aber effizient für den Aufbau eines Compliance-Management-Systems einsetzt indem man Thema nach Thema angeht. Dabei kommt es einem auch zugute, dass man aus der

Erfahrung der Umsetzung der ersten Themen lernt und diese auf die weitere Implementierung eines Compliance-Management-Systems übertragen kann.

Die Ausrichtung eines Compliance-Management-Systems bestimmt sich aus mehreren Perspektiven: Anforderungen an Compliance können extern über gesetzliche Anforderungen (etwa dem UK *Bribery Act*), über Geschäftspartner (z.B. Kunden), Kapitalgeber (vielleicht Venture Capital Provider, die darauf angewiesen sind, Unternehmensanteile nach einer gewissen Zeit wieder zu vermarkten und daher Wert auf bestimmte Compliance-Ziele legen), aber auch intern aufgrund von Vorfällen im Unternehmen oder Wertvorstellungen der Unternehmensinhaber, Geschäftsleitungen und auch der Belegschaft an ein Unternehmen herangetragen werden.

Bei der Zieldefinition sollte man sich schon Gedanken über die Zielerreichung und mögliche Maßnahmen der Umsetzung machen. Hehre Postulate können verhallen, wenn sie keinen Bezug auf den Geschäftsbetrieb und die Geschäftsstrategie haben. Ambitiöse Wachstumsziele vertragen sich nur dann mit anspruchsvollen Integritätszielen, wenn hier von Anfang an eine Symbiose gesucht wird und die Ziele auf einer Ebene konkretisiert werden, dass mögliche Widersprüche aufgelöst werden. Passen Geschäfts- und Integritätsziele nicht zusammen, so zeigt sich erste Kritik an einem Compliance-Management-System durch Zweifel bis hin zur mangelnden Glaubwürdigkeit bei Belegschaft und Kunden. Ziele müssen als erstes dem kritischen Blick relevanter Funktionsträger standhalten können, nur dann werden sie auch erfüllbar sein.

6.2 Compliance-Risiko

Eine Risikoanalyse kann einer Zieldefinition bereits vorausgehen, insbesondere dann, wenn ein Unternehmen seine Ziele dem tatsächlichen Bedarf nach ausrichten will und hierzu zunächst eine Bestandsaufnahme durchführt. Nicht immer wird ein bestehendes Risikomanagement alle möglichen Compliance-Themen im Blick haben, sinnvoll ist es jedoch, bereits vorhandene Risikoübersichten mit einzubeziehen (z.B. Lageberichte, Risikostudien oder Revisionsberichte). Allerdings wird man die Risikoanalyse nach einer Zielfestlegung darauf ausgerichtet vertiefen müssen. Es gilt solche Risiken zu erkennen, die die Zielerreichung insgesamt in Frage stellen können. Hier müssen entsprechende Maßnahmen ansetzen, will man beim Aufbau eines wirkungsvollen Compliance-Management-Systems auch erfolgreich sein.

Eine nachgelagerte Risikoanalyse hilft jedoch, die definierten Compliance-Ziele zu verifizieren und – sofern ein stufenweises Vorgehen erwünscht ist – Gefährdungspotentiale zu erkennen und entsprechend anzugehen. Dabei ist eine Abwägung von Eintritts- und Auswirkungswahrscheinlichkeiten vorzunehmen. Eine Risikoanalyse kann auf vielfältige Weise durchgeführt werden. Eine rein theoretische Risikobetrachtung, ausgehend von Branchen- und Industrieerfahrungen kann eine gute Einleitung sein. Auch vielfältig von internationalen Organisationen, Branchendiensten, Unternehmensberatungen und Behörden bereitgestellte Informationssammlungen und Indizes erlauben eine erste Risikoeinschätzung. Neben bestehenden Informations-

quellen im Unternehmen, die über die Berichtslage auswertbar sind, helfen Workshops oder Einzelgespräche mit Mitarbeitern in Schlüsselpositionen. Schließlich können in Einzelfällen auch gelenkte Dokumentenreviews sinnvoll sein. Eine Risikoanalyse sollte nicht in voller Breite einen Zustandsbericht über das gesamte Unternehmen anstrengen, sondern zielgerichtet und gelenkt von einer ersten Risikoübersicht seitens der Geschäftsleitung, der Revisions- und Rechtsabteilung zu den Führungskräften sensibler Abteilungen (z. B. Vertrieb und Einkauf) bis hin zur Detailbefragung von Personen in Schlüsselpositionen (wie etwa in der Strategie, im Support oder im Qualitätsmanagement) ausgerichtet. Stichproben in die Dokumentation typischer Geschäftssituationen können eine Risikoanalyse abschließen. Hier ist schon ein Blick in Geschäftsprozesse und -abläufe möglich, der bereits die Maßnahmenplanung einleiten hilft.

Für eine spätere IDW-Prüfung sollte allerdings die Methodik und die Vorgehensweise bei der Risikoanalyse festgehalten werden. Die Ergebnisse der Risikoanalyse müssen nachvollziehbar sein. Insbesondere für die Geschäftsleitung kann der Nachweis einer validen Vorgehensweise bei der Risikobetrachtung und der Planung des späteren Compliance-Programms entlastend wirken, so etwa wenn bei einer Risikoanalyse mit externer Begleitung die Eintrittswahrscheinlichkeit eines Risikos als gering eingeschätzt und Compliance-Maßnahmen zurückgestellt werden,

dann sich aber das Risiko wider Erwarten unmittelbar verwirklicht hat. Wenn hier ein methodisch ordnungsgemäßes und auch geprüftes Vorgehen darstellbar ist, wird sich eine Geschäftsleitung kaum den Vorwurf mangelnder Aufsicht nach § 130 OWiG aussetzen lassen müssen.

Die Risikoanalyse zeigt, welche Maßnahmen erforderlich sind und welche organisatorischen Vorkehrungen nach Qualität und Quantität getroffen werden müssen, um die gesetzte Compliance-Ziele realistisch erfüllen zu können. Die Risikoanalyse erlaubt auch den effektiven Einsatz der regelmäßig beschränkten Ressourcen für ein Compliance-Management-System.

6.3 Compliance-Programm

Die auf die Zieldefinition aufbauende oder daran angepasste Risikoanalyse wird regelmäßig einen Handlungsbedarf erkennen lassen. Dieser ist in einer Vorgehensplanung zu erfassen und bildet die



Basics für die Spitze

Grundlagen der Unternehmensführung Einführung in die Managementlehre

Von Prof. Dr. Fred G. Becker

2011, 307 Seiten, mit zahlreichen Abbildungen, € (D) 24,95,
ISBN 978-3-503-13663-6

Weitere Informationen:

 www.ESV.info/978-3-503-13663-6

ESV

ERICH SCHMIDT VERLAG
Auf Wissen vertrauen

Bestellungen bitte an den Buchhandel oder: Erich Schmidt Verlag GmbH & Co. KG · Genthiner Str. 30 G
10785 Berlin · Fax 030/25 00 85-275 · Tel. 030/25 00 85-265 · ESV@ESVmedien.de · www.ESV.info

ESV
basics

Grundlage des Compliance-Programmes zum Aufbau eines Compliance-Management-Systems. Dabei ist das Compliance-Programm das Maßnahmenpaket zum Aufbau eines Compliance-Management-Systems und zur Umsetzung der Compliance-Ziele.

Die Maßnahmen können höchst unterschiedlich sein: Vorgaben und Handlungsempfehlungen in der Form von Richtlinien, Stellungnahmen oder gar Anweisungen – bis hin zu Elementen innerhalb von Geschäftsabläufen (z. B. IT-Order-Systemen u. a.), die helfen sollen, Compliance in der täglichen Geschäftstätigkeit zu verankern. Bei den Maßnahmen wird sich das Compliance-Management-System regelmäßig unternehmensspezifisch individualisieren.

6.4 Compliance-Organisation

Ebenfalls individuell auf das Unternehmen und seine Organisation zugeschnitten wird auch eine Compliance-Organisation anzulegen sein. Wichtig ist, dass eine zentrale Funktion für Compliance besteht (Compliance-Officer, Compliance-Manager oder Compliance-Beauftragter). Dabei ist diese Funktion nicht dafür verantwortlich, dass Compliance im Unternehmen „herrscht“, sondern muss die Aufsichtsfunktion nach § 130 Abs. 1 OWiG erfüllen, und dafür Sorge tragen, dass ein Compliance-Management-System hinreichend organisiert ist, um mindestens Straftaten oder Ordnungswidrigkeiten zu verhindern helfen. Nur dann kann sich eine Geschäftsleitung sicher sein, dass eine Compliance-Organisation sie von ihrer umfangreichen Verantwortung entlastet, wenn sie dazu funktionell, personell, ressourcenmäßig und auch fachlich in der Lage ist, diese Aufgabe zu übernehmen.

Ob nun ein *Chief Compliance-Officer* oder ein *Compliance-Committee* aus dem Leiter der Rechtsabteilung, der Revision, der Personalabteilung oder des Risikomanagements und anderer Unternehmensbereiche diese Verantwortung von der Geschäftsleitung übernehmen, ist dann unerheblich, wenn effektiv ein Compliance-Management-System umgesetzt wird. Eine Verankerung von Compliance unmittelbar im Vorstand mag vorteilhaft für das Auftreten von Compliance insbesondere

in der Öffentlichkeit sein – die Verantwortung jedoch verbleibt kollektiv im Vorstand oder Geschäftsführung. Eine Compliance-Funktion unterhalb der Ebene der Geschäftsleitung eröffnet die Möglichkeit der Delegation und damit der Entlastung der Geschäftsleitung.

6.5 Compliance-Kommunikation

Eines der wesentlichsten Handlungsfelder eines Compliance-Management-Systems ist das der Kommunikation. Nicht von ungefähr stellen sowohl die US-FSGO als auch die britische *Guidance* Kommunikation und Schulung in besonderer Weise aus dem Kreis der erforderlichen Compliance-Maßnahmen heraus. Dabei geht es nicht um reine Informationsvermittlung von Gesetzestexten, unternehmensinternen Stellungnahmen, Anweisungen, Richtlinien oder Schulungsunterlagen bis hin zu eLearning Programmen. Es geht hier um nichts Geringeres als die Vermittlung der Unternehmenskultur an alle Mitarbeiter und Geschäftspartner eines Unternehmens. Die Compliance-Kommunikation muss dafür Sorge tragen, dass das gesamte Unternehmen auf die festgelegten Compliance-Ziele hin ausgerichtet wird und sich alle Betroffenen an der Erreichung dieser Ziele nach besten Kräften beteiligen. Dabei sind auch die weiteren, im Sinne des Geschäftserfolges wichtigen, eigentlichen Unternehmensziele in gleicher Weise zu beachten und zu ermitteln.

Wirkungsvolle Kommunikation orientiert sich am Empfänger und der Frage, wie und auf welche Weise kann der Empfänger die gesetzten Compliance-Ziele erreichen. Neben den Mitarbeitern und Geschäftspartnern müssen auch weitere Empfängerhorizonte erreicht werden: Gegenüber den Kunden und der breiten Öffentlichkeit ist die Reputation des Unternehmens zu steuern. Aktionäre, Kapitalgeber, Zulieferer, Meinungsbilder und andere *stakeholder* sind im Sinne von Compliance für das Unternehmen anzusprechen. Hier gilt es Erwartungen an das Unternehmen allgemein und gerade im Hinblick auf Compliance zu erfüllen. Erfolgreich kann die Kommunikation hier nur sein, wenn es ihr gelingt, alle Betroffenen für das Unternehmen und seine Integrität wie auch wegen seiner Integrität einzusetzen. So ist es möglich, durch ein wirkungsvolles Compliance-Management-System auch Wettbewerbsvorteile zu schaffen und Integritäts- sowie wirtschaftliche Unternehmensziele miteinander wirkungsvoll zu verbinden.

Dabei ist jeder Schritt beim Aufbau eines Compliance-Management-Systems schon hinsichtlich der Kommunikation sorgfältig zu planen. Kommunikation beginnt schon bei der Risikoanalyse. Oft ist der Workshop oder das Gespräch der erste Kontakt der Mitarbeiter mit dem Thema Compliance. Wenn es hier nicht gelingt, von Anfang an Compliance als Support-Funktion zur Unterstützung eines regelgerechten Verhaltens zu etablieren, sind spätere Schwierigkeiten bei dem Erreichen der gesetzten Compliance-Ziele vorauszusehen.

6.6 Überwachung und Verbesserung

Vollständig ist ein Compliance-Management-System erst, wenn es selbst auch seine eigene Effektivität und Effizienz prüfen und mit darauf aufbauenden Optimierungsmaßnahmen stets auf

einem aktuellen und auch wirkungsvollen Stand bleiben kann. Ermittlungs- und Aufsichtsbehörden akzeptieren, dass nicht jeder Compliance-Verstoß verhindert werden kann. Kriminelle Fantasie wird aber immer wieder Wege finden, auf rechtswidrige Weise persönliche Vorteile zu erlangen. Auch neue Entwicklungen im Unternehmen sowie neue Geschäftsstrategien führen immer wieder zu stets neu zu bewältigenden Anforderungen für Compliance. Oft entstehen dann Defizite, wenn bestehende und bewährte Risikomanagementsysteme nicht mehr an aktuelle Gegebenheiten angepasst werden. Hier bedarf es der Aufmerksamkeit gegenüber weiteren Anforderungen sowohl unternehmensimmanent als auch von Außen (z.B. aus der Entwicklung der Gesetzgebung), den kritischen Blick auf mögliche Defizite des bestehenden Systems (z.B. erkannte Schwächen) und auch auf Neuentwicklungen in der Wirtschaft (etwa über ein *Peer-Review* oder *Benchmarking* gegenüber anderen Unternehmen).

In dem Element der Überwachung und Verbesserung liegt noch ein erhebliches Handlungspotential. Mittlerweile haben viele Unternehmen Compliance-Organisationen eingerichtet, die auch den derzeitigen Stand des Risikomanagements beachten, ein regelmäßiger Test auf Effektivität und Effizienz findet (noch) nicht statt. Dabei sollte schon von Anfang an, mit der ersten Umsetzung von Maßnahmen eines Compliance-Programms geprüft werden, ob die Maßnahmen überhaupt tauglich sind, Compliance-Risiken einzudämmen und die gesetzten Zielvorgaben auch zu erreichen. Oft werden Maßnahmen umgesetzt, die für andere Unternehmen entwickelt oder aber aus Dringlichkeitsgründen eher vorläufig angesetzt wurden. Hier ist es nun die Prüfung erforderlich, ob tatsächlich die erwünschte Wirkung im Unternehmen eingesetzt hat. Diese Prüfung sollte man nicht dem Zufall und dem möglichen Eintritt einer Compliance-Krise überlassen.

Ein kritischer Blick auf die eigenen Compliance-Maßnahmen schafft zum einen neue Erkenntnisse über selbst periphere Bereiche des eigenen Unternehmens und lässt schnell erkennen, welche Ansätze zur Verankerung von Regeltreue erfolgreich und welche verbesserungsbedürftig sind. Eine frühe Prüfung parallel zu ersten Implementierungsmaßnahmen verhindert oder vermindert zudem den verlorenen Aufwand für die Umsetzung ganz oder teilweise untauglicher Maßnahmen. Hilfreich sind hier Stichprobenprüfungen, bei denen man sich bewusst auf einzelne Funktionen innerhalb von lokalen oder zentralen Geschäftsbereichen beschränkt.

Eine systematische Überwachung der Umsetzung des Compliance-Programms etwa mit einem Prüfungsplan erlaubt zudem eine aktuelle Ergänzung der Risikoanalyse und führt schon so automatisch zu einer steten Aktualisierung des Compliance-Programms. Auf diese Weise entsteht ein Überblick über den Erfolg des Compliance-Management-Systems. Sowohl die Compliance-Organisation als auch die einzelnen Einheiten sowie die Geschäftsleitung haben einen Überblick über den Status von Compliance im Unternehmen und können entsprechend eingreifen. Nichts anderes verlangt § 130 OWiG.

7. Fazit

Die Prüfung des betrieblichen Compliance-Management-Systems ist eine Option, die nach § 130 OWiG von der Geschäftsleitung geforderten Aufsicht über Maßnahmen zur Verhinderung von Straftaten und Ordnungswidrigkeiten umzusetzen. Sie ermöglicht den externen, standardisierten, kritischen Blick auf das Compliance-Management-System des Unternehmens. Der Standard gibt wesentliche Elemente eines solchen Systems wieder. Er lässt dabei den Unternehmen größtmögliche Flexibilität bei der Ausgestaltung und Umsetzung. Die Prüfung verifiziert, ob die Elemente in ausreichender und spezifisch auf das Unternehmen angepasster Weise ausgeführt wurden und eine Grundlage für ein effektives Management insbesondere rechtlicher Risiken bieten können. Man muss nicht auf einen Vorfall warten, um die eigene Risikoversorge zu testen. Die Prüfung nach IDW PS 980 eröffnet rechtzeitig Handlungsspielräume zum Schutz des Unternehmens, seiner Geschäftsleitung und Mitarbeiter.

In den nächsten Heften wird die ZRFC einzelne Compliance-Themen vorstellen und Beispiele zeigen, wie ein entsprechendes Compliance-Management-System gestaltet und aufgebaut werden kann.